ら

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/697,641	10/31/2003	Bernd Labertz	1509-452	8476

22879   7590   03/21/2007
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
SHIN, KYUNG H

ART UNIT	PAPER NUMBER
2143	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

PTOL-90A (Rev. 10/06)

	Application No.	Applicant(s)
Office Action Summary	10/697,641	LABERTZ, BERND
	Examiner	Art Unit	
	Kyung H. Shin	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>31 October 2003</u>.

2a) ☐ This action is **FINAL.**   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-24</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-24</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on <u>10/31/03</u> is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date <u>8/21/06</u>

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   This action is responding to application filed on **10-31-2003**, and FOREIGN

PRIORITY date is **8-11-2003**.

2.   Claims **1 - 24** are pending. Claim **1, 7, 10, 12, 14, 17, 21, 23** are independent.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.   .

4.   Claim **1 - 11, 14 - 24** are rejected under 35 U.S.C. 102(e) as being anticipated by

Douglas (US PGPUB No. **20040049693**).

Regarding Claim 1, Douglas discloses a method of monitoring a plurality of local event

logs of a computer network, the method comprising:

   a) entering the local event logs in a central database of the computer network, (see

       Douglas paragraph [0004], lines 3-13: event processing; paragraph [0040], lines

       5-8; paragraph [0080], lines 1-6: central database; paragraph [0031], lines 16-18;

       paragraph [0071], lines 1-12: storage event logs) and

b) sending the central database from the computer network to an external support

computer system for analysis of the local event logs. (see Douglas paragraph

[0022], lines 14-18; paragraph [0024], lines 11-13; paragraph [0024], lines 16-18:

transfer external system (i.e. aggregated events), event log analysis)

Regarding Claim 2, Douglas discloses the method of claim 1, wherein each local event

log is generated for one particular node of the computer network, and storing the local

event logs in the central database using a corresponding node identifier as a key. (see

Douglas paragraph [0031], lines 16-18; paragraph [0071], lines 1-12; paragraph [0040],

lines 5-8; paragraph [0080], lines 1-6: storage event logs (i.e. database); paragraph

[0082], lines 1-8: record (i.e. event record) identifier)

Regarding Claim 3, Douglas discloses the method of claim 1, the computer network

comprising a server computer for storing the central database, the server computer

having a local server event log, the method further comprising storing the local server

event log in the central database, and sending the central database from the server

computer of the computer network to the external support computer system. (see

Douglas paragraph [0020], lines 1-3; paragraph [0021], lines 9-12: HIDS, NIDS servers,

central database; paragraph [0031], lines 16-18; paragraph [0071], lines 1-12: storage

event logs; paragraph [0022], lines 14-18; paragraph [0024], lines 11-13; paragraph

[0024], lines 16-18: transfer to external support system (i.e. aggregated events))

Regarding Claim 4, Douglas discloses the method of claim 3, further comprising

entering an event into the local server event log after the central database has been

sent to the external support computer system. (see Douglas paragraph [0032], lines 2-3:

continuous (i.e. no termination) event logging, even after transfer to external system)

Regarding Claim 5, Douglas discloses the method of claim 1, wherein each event log

entry in a local event log has an event identifier, a time stamp and event information

descriptive of the event. (see Douglas paragraph [0082], lines 1-8: record identifier;

paragraph [0184], lines 1-2; paragraph [0184], lines 9-11: event record, date/time (i.e.

time stamp), description of event)

Regarding Claim 6, Douglas discloses the method of claim 1, wherein the central

database is stored on a server computer of the computer network, and further

comprising the steps of:

a) coupling program code from the server computer to network nodes of the

    computer network, (see Douglas paragraph [0003], lines 1-13: software, program

    code; paragraph [0004], lines 3-5: access to distributed network nodes (i.e.

    coupled to network)) and

b) transferring the local event logs of the network nodes to the server computer by

    remotely executing the program code by the server computer on the network

    nodes. (see Douglas paragraph [0003], lines 1-13: software, program code;

paragraph [0004], lines 9-13: transfer event log (i.e. aggregated events)

information to server)

Regarding Claim 7, Douglas discloses a memory storing a computer program for

causing a computer network to generate a central database for storing local event logs

of network nodes of the computer network, the computer program causing the computer

network to perform the steps of:

a) transmitting the respective local event logs from the network nodes to a server

computer of the computer network, (see Douglas paragraph [0004], lines 9-13:

local event logs (i.e. aggregated events) transferred to server)

b) storing the local event logs in the central database on the server computer using

the node identifiers of the network nodes as keys for the respective local event

logs, (see Douglas paragraph [0040], lines 5-8; paragraph [0080], lines 1-6;

paragraph [0027], lines 8-10: storage, central server database; paragraph [0082],

lines 1-8: event record identifier (i.e. key to retrieve event record)) and

c) storing a local server event log of the server computer in the central database,

the local server event log being adapted to store a send event after the central

database has been sent to an external support computer system for analysis of

the local event logs. (see Douglas paragraph [0024], lines 11-13; paragraph

[0024], lines 16-18: transfer to external support system (i.e. aggregated events)

for analysis)

Regarding Claim 8, Douglas discloses the memory of claim 7, wherein the program

causes the network to send the central database to the external support computer

system at customisable periodic time intervals. (see Douglas paragraph [0032], lines 1-

2; paragraph [0032], lines 5-6; paragraph [0032], lines 8-10: timed interval for

monitoring, event logs, schedule setup (i.e. customizable))

Regarding Claim 9, Douglas discloses the memory of claim 7, wherein the program

includes program code for remote execution on the network nodes to cause the network

nodes to send the respective local event logs to the server computer. (see Douglas

paragraph [0003], lines 1-13: software, program code; paragraph [0004], lines 9-13:

event logs (i.e. aggregated events) transferred to server)

Regarding Claim 10, Douglas discloses a server computer system of a computer

network having a plurality of network nodes, the server computer system comprising:

    a) a controller for causing the network nodes to transmit respective local event logs

       of the network nodes to the server computer system, (see Douglas paragraph

       [0004], lines 9-13: transfer (i.e. network communications) event logs to server)

    b) a store for the local event logs in a central database, (see Douglas paragraph

       [0040], lines 5-8; paragraph [0080], lines 1-6: central database; paragraph

       [0031], lines 16-18; paragraph [0027], lines 8-10: storage event logs)

    c) a transmitter for sending the central database to an external support computer

       system for analysis of the local event logs. (see Douglas paragraph [0024], lines

11-13; paragraph [0024], lines 16-18: transfer to external support system (i.e.

aggregated events), event logs analysis)

Regarding Claim 11, Douglas discloses the server computer system of claim 10,

further comprising a local server event log for storing an event in response to the central

database being sent to the external support computer system, the send event having a

time stamp. (see Douglas paragraph [0184], lines 1-2; paragraph [0184], lines 9-11:

event log record, event record (i.e. including send event), data/time (i.e. timestamp))

Regarding Claim 14, Douglas discloses a method of monitoring a plurality of local

event logs, the method comprising the steps of:

a) receiving a database from a customer computer network, the database

    comprising the local event logs of network nodes of the computer network, (see

    Douglas paragraph [0022], lines 14-18; paragraph [0024], lines 11-13; paragraph

    [0024], lines 16-18: transfer external system (i.e. aggregated events), event logs

    analysis, transfer/receive)

b) querying the database to identify a database send event in the local event logs

    and its corresponding sent time stamp, (see Douglas paragraph [0040], lines 5-8;

    paragraph [0080], lines 1-6: query (i.e. database command), record(s) within

    database; paragraph [0184], lines 1-2; paragraph [0184], lines 9-11: database

    records with data/time (i.e. timestamp))

c) querying the database to identify local event log entries having time stamps later

than the sent time stamp. (see Douglas paragraph [0040], lines 5-8; paragraph

[0080], lines 1-6: query (i.e. database command), record(s) within database

timestamp part of record, compare time stamps)

Regarding Claim 15, Douglas discloses the method of claim 14, further comprising

comparing the identified event log entries to rules of alert policies to determine whether

an alert action should be invoked. (see Douglas paragraph [0022], lines 14-15;

paragraph [0066], lines 1-5; paragraph [0218], lines 2-4: security policy (i.e. rules),

process event log to generate alert)

Regarding Claim 16, Douglas discloses the method of claim 15, further comprising

sending an email message to a response center engineer as an alert action. (see

Douglas paragraph [0020], lines 3-6; paragraph [0028], lines 1-4: e-mail alert, event log

processed)

Regarding Claim 17, Douglas discloses a memory storing a computer program for

enabling a computer to monitor plural local event logs of a computer network, the

computer program causing the computer to perform the steps of:

a) storing a database associated with a customer computer network, the database

comprising the local event logs of network nodes of the computer network, (see

Douglas paragraph [0040], lines 5-8; paragraph [0080], lines 1-6: central

database; paragraph [0027], lines 8-10; paragraph [0031], lines 16-18: storage

event logs; paragraph [0003], lines 1-13: software, program)

b) querying the database to identify a database send event in the local event logs

and its corresponding sent time stamp, (see Douglas paragraph [0040], lines 5-8;

paragraph [0080], lines 1-6: database, query (i.e. database command), record(s)

within database: query (i.e. database command), record(s) within database,

timestamp part of record, check time stamps; paragraph [0184], lines 1-2;

paragraph [0184], lines 9-11: database records with data/time (i.e. timestamp))

and

c) querying the database to identify local event log entries having time stamps later

than the sent time stamp. (see Douglas paragraph [0040], lines 5-8; paragraph

[0080], lines 1-6: central database, query (i.e. database command), record(s)

within database, timestamp part of record, compare time stamps)

Regarding Claim 18, Douglas discloses the memory of claim 17, wherein the program

causes the computer to determine whether an alert action should be invoked by

comparing the identified event log entries to rules of alert policies. (see Douglas

paragraph [0022], lines 14-15; paragraph [0066], lines 1-5; paragraph [0218], lines 2-4:

security policy (i.e. rules), process event log to generate alert; paragraph [0003], lines 1-

13: software, program code)

Regarding Claim 19, Douglas discloses the memory of claim 18, wherein the program

causes the computer to send an automatic notification to a response center engineer if

the determining step determines an alert action should be invoked. (see Douglas

paragraph [0020], lines 3-6; paragraph [0028], lines 1-4: automatic e-mail alert sent,

event log processed; paragraph [0003], lines 1-13: software, program code)

Regarding Claim 20, Douglas discloses the memory of claim 17, wherein the computer

program causes the computer to receive from the customer computer network the

database associated with the customer computer network. (see Douglas paragraph

[0003], lines 1-13: software, program code; paragraph [0024], lines 11-13; paragraph

[0024], lines 16-18: transfer database over customer computer network)

Regarding Claim 21, Douglas discloses a support computer system for providing

network support services for a customer computer network, the support computer

system comprising:

a) a memory for storing a database associated with the customer computer

network, the database comprising local event logs of network nodes of the

customer computer network, (see Douglas paragraph [0027], lines 8-10: event

log information stored (memory, disk storage); paragraph [0040], lines 5-8;

paragraph [0080], lines 1-6: database)

b) a database query component for querying the database to determine a database

send event and its corresponding transfer time stamp in the database and for

querying the database to identify event log entries having time stamps later than

the sent time stamp, (see Douglas paragraph [0040], lines 5-8; paragraph [0080],

lines 1-6: database, query (i.e. database command); paragraph [0184], lines 1-2;

paragraph [0184], lines 9-11: database records with data/time (i.e. timestamp))

c) an analysis component for comparing the identified event log entries to the rules

of alert policies to determine whether an alert action should be invoked. (see

Douglas paragraph [0022], lines 14-15; paragraph [0066], lines 1-5; paragraph

[0218], lines 2-4: security policy (i.e. rules), process event log to generate alert)

Regarding Claim 22, Douglas discloses a system according to claim 21 wherein the

memory is adapted to receive from the customer's computer network the database

associated with the customer computer network. (see Douglas paragraph [0024], lines

11-13; paragraph [0024], lines 16-18: transfer database (i.e. aggregated events) over

customer computer network)

Regarding Claim 23, Douglas discloses a response center computer system for

providing network support services for a plurality of customer computer networks, the

response center computer system comprising:

a) a memory for storing a database associated with the customer computer

network, the database comprising local event logs of network nodes of the

customer computer network, (see Douglas paragraph [0027], lines 8-10: storage

of event logs (i.e. hard disk, memory), database)

b) a database query component for querying the database to determine a database

send event and its corresponding transfer time stamp in the database and for

querying the database to identify event log entries having time stamps later than

the sent time stamp, (see Douglas paragraph [0040], lines 5-8; paragraph [0080],

lines 1-6: database, query (i.e. database command), record(s) within database:

query (i.e. database command), record(s) within database, timestamp part of

record, compare time stamps; paragraph [0184], lines 1-2; paragraph [0184],

lines 9-11: database records with data/time (i.e. timestamp))

c) an analysis component for comparing the identified event log entries with rules of

alert policies to determine whether an alert action should be invoked, (see

Douglas paragraph [0022], lines 14-15; paragraph [0066], lines 1-5; paragraph

[0218], lines 2-4: security policy (i.e. rules), process event log to generate alert)

and

d) an automatic notification component for sending an email message to a response

center engineer in response to the analysis component determining that an alert

action should be invoked. (see Douglas paragraph [0020], lines 3-6; paragraph

[0028], lines 1-4: e-mail alert, event log processed)

Regarding Claim 24, Douglas discloses a system according to claim 23 wherein the

memory is adapted to receive from the customer's computer network the database

associated with the customer computer network. (see Douglas paragraph [0024], lines

11-13; paragraph [0024], lines 16-18: transfer database (i.e. aggregated events) over

customer computer network)

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims **12, 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over

Douglas in view of **Katz et al.** (US PGPUB No. **20020062259**).

Regarding Claim 12, Douglas discloses a server comprising:

   b) a remote execution program component for causing the network nodes to

      transmit respective local event logs to the server, (see Douglas paragraph

      [0003], lines 1-13: software, execution program (i.e. local, remote))

   d) an interface component for sending the central database to the external support

      computer system for analysis of the local event logs. (see Douglas paragraph

      [0003], lines 1-4: interface component, network communications)

      Douglas discloses a central database for storing the local event logs and for

      storing a local server event log, and a program performing functions. (see

Douglas paragraph [0004], lines 3-5: event log processing; paragraph [0003],

lines 1-13: software, program)   Douglas does not specifically disclose a

discovery server system.

However, Katz discloses wherein:

a) a discovery component for discovery of network nodes of a computer network,

(see Katz paragraph [0023], lines 1-5: event processing; paragraph [0068], lines

1-4; paragraph [0068], lines 9-13: discovery capability for network nodes)

c) a local discovery server, (see Katz paragraph [0023], lines 1-5: event processing;

paragraph [0068], lines 1-4; paragraph [0068], lines 9-13: discovery capability for

network nodes)

It would have been obvious to one of ordinary skill in the art to modify Douglas

as taught by Katz to enable the capability to utilize a server system with a discovery

function. One of ordinary skill in the art would have been motivated to employ the

teachings of Katz in order to enhance event processing capabilities by increasing

event types for event log processing by the addition of device generated events.

(see Katz paragraph [0016], lines 4-9: " ... *It is also desirable to provide systems that*

enable and facilitate the initiation of data transfer, e-commerce and other digital

transactions, responsive to device generated events, which may be generated, for

example, at device installation or removal, or at other times during device operation.

... ")

Regarding Claim 13, Douglas discloses the discovery server of claim 12, wherein the local discovery server event log is adapted to store an event indicative of a transfer of the central database from the server to the external support computer system. (see Douglas paragraph [0004], lines 3-5: event log processing; paragraph [0040], lines 5-8; paragraph [0080], lines 1-6: database; paragraph [0022], lines 14-18; paragraph [0024], lines 11-13; paragraph [0024], lines 16-18: transfer external system)   Douglas does not specifically disclose a discovery server.   However, Katz discloses wherein a discovery server.   (see Katz paragraph [0023], lines 1-5: event processing; paragraph [0068], lines 1-4; paragraph [0068], lines 9-13: discovery capability for network nodes)

It would have been obvious to one of ordinary skill in the art to modify Douglas as taught by Katz to enable the capability utilize a server system with a discovery function. One of ordinary skill in the art would have been motivated to employ the teachings of Katz in order to enhance event processing capabilities by increasing event types for event log processing by the addition of device generated events.   (see Katz paragraph [0016], lines 4-9)

Conclusion

7.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H. Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9:30 am - 6 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number

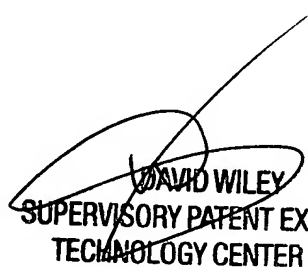for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

K H S
Kyung H Shin
Patent Examiner
Art Unit 2143

***

KHS
March 10, 2007

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100